# Bug 2430781 (CVE-2026-1180) - CVE-2026-1180 org.keycloak.protocol.oidc: Blind Server-Side Request Forgery (SSRF) in Keycloak OIDC Dynamic Client Registration via jwks_uri

**Keywords:** Security ×

**Status:** NEW

**Alias:** CVE-2026-1180

**Product:** Security Response

**Component:** vulnerability

**Version:** unspecified

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**

**TreeView+** depends on / blocked

**Reported:** 2026-01-19 07:41 UTC by OSIDB Bzimport

**Modified:** 2026-02-18 08:27 UTC (History)

**CC List:** 26 users (show)

**Fixed In Version:**

**Clone Of:**

**Environment:**

**Last Closed:**

**Embargoed:**

---

**Attachments** (Terms of Use)

OSIDB Bzimport 2026-01-19 07:41:58 UTC Description

```
Blind Server-Side Request Forgery (SSRF) vulnerability in the
Keycloak OIDC Dynamic Client Registration flow when using
private_key_jwt client authentication. The flaw is caused by
the absence of validation or restriction on the jwks_uri
parameter supplied during client registration. When validating
a client’s JWT assertion, Keycloak automatically fetches the
JWKS from the attacker-controlled URI using server-side HTTP
requests. This allows remote attackers to force the Keycloak
server to access internal network resources such as localhost
services, RFC1918 addresses, or cloud metadata endpoints.
Although responses are not directly returned, attackers can
infer reachable services via timing and error behavior,
```

enabling internal network enumeration without authentication in configurations that permit anonymous or token-based client registration.

Note

You need to log in before you can comment on or make changes to this bug.